Oracle Enterprise Session Border Controller with Anynode UCMA and Microsoft's Online Exchange Unified Messaging (Office 365 ExUM)

Technical Application Note

Disclaimer

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

Table of Contents

Intended Audience

This document is intended for use by Oracle Systems Engineers, third party Systems Integrators, and end users of the Oracle Enterprise Session Border Controller (E-SBC). It assumes that the reader is familiar with basic operations of the Oracle Enterprise Session Border Controller.

Document Overview

The following document shares technical information pertaining to integration guidelines recommended for smooth interop between Oracle ESBC, Microsoft Office 365 & TE-Systems Anynode.

Introduction

Audience

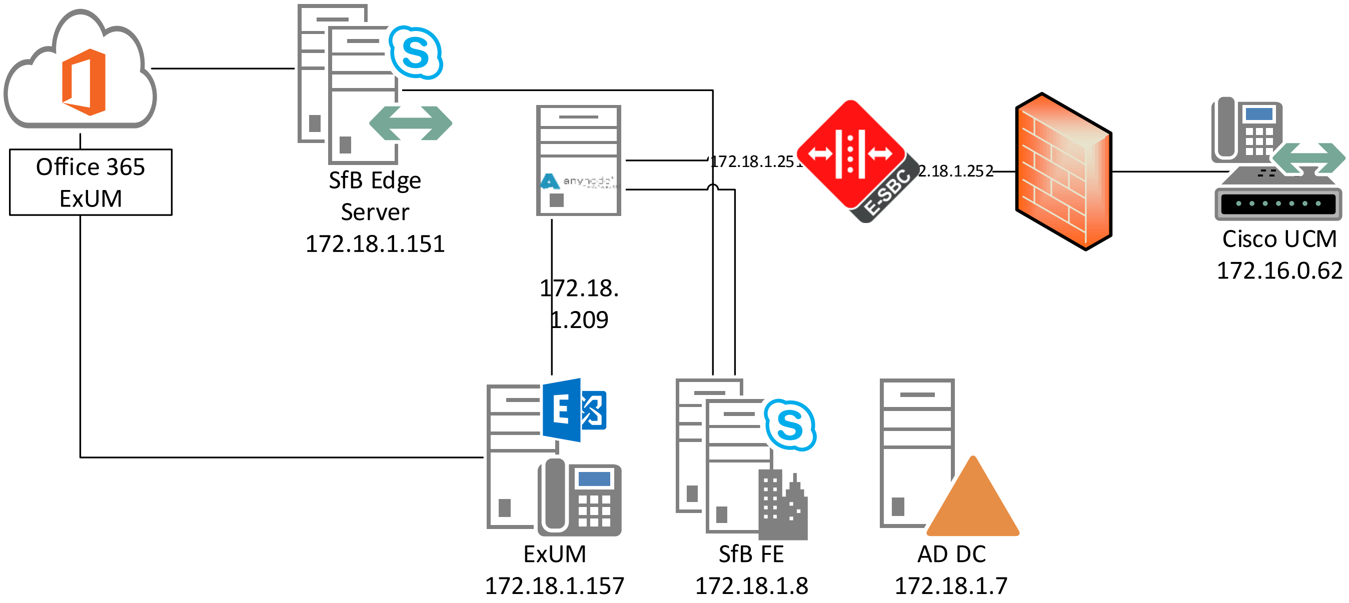
This is a technical document intended for telecommunications engineers with the purpose of configuring the Oracle Enterprise Session Border Controller and Anynode's UCMA SBC. There will be steps that require navigating the Command Line Interface (ACLI). Understanding the basic concepts of TCP/UDP, IP/Routing, SIP/RTP, TLS and SRTP are also necessary to complete the configuration and for troubleshooting, if necessary.

Requirements

- Anynode - 3.7.50
- Oracle Enterprise Session Border Controller is running ECZ7.5.0 Patch 3

Architecture

The following reference architecture shows a logical view of the connectivity



Lab Configuration

Following are the IP addresses used for the Interoperability tests. The IPs below are specific to lab setup at Completely, the IPs in production will be vastly different from network addresses listed below.

Hostname / IP address:

- 172.16.1.245 (wancom0 / management)
- 172.18.1.251 (outside realm) connected to anynode (172.18.1.209:5062)
- 172.18.1.252 (inside realm) connected to Cisco UCM (172.16.0.62:5060)

Configuring the Oracle Enterprise Session Border Controller

In this section we describe the steps for configuring an Oracle Enterprise Session Border Controller, formally known as an Acme Packet Net-Net Enterprise Session Director, for use with CIC Server in a SIP trunking scenario.

In Scope

The following guide configuring the Oracle E-SBC assumes that this is a newly deployed device dedicated to a single customer. If a service provider currently has the E-SBC deployed then please see the ACLI Configuration Guide on http://docs.oracle.com/cd/E56581_01/index.htm for a better understanding of the Command Line Interface (CLI).

Note that Oracle offers several models of E-SBC. This document covers the setup for the E-SBC platform running ECZ7.3.0 or later. If instructions are needed for other Oracle E-SBC models, please contact your Oracle representative.

Out of Scope

- Configuration of Network management including SNMP and RADIUS

What will you need

- Hypervisor with console connectivity through the hypervisor
- Terminal emulation application such as PuTTY or HyperTerm
- Passwords for the User and Super user modes on the Oracle E-SBC
- IP address to be assigned to management interface (Wancom0) of the E-SBC - the Wancom0 management interface must be connected and configured to a management network separate from the service interfaces. Otherwise the E-SBC is subject to ARP overlap issues, loss of system access when the network is down, and compromising DDoS protection. Oracle does not support E-SBC configurations with management and media/service interfaces on the same subnet.
- IP address of CIC external facing NIC
- IP addresses to be used for the E-SBC internal and external facing ports (Service Interfaces)
- IP address of the next hop gateway in the service provider network

Configuring the E-SBC

Enter the following commands to login to the E-SBC and move to the configuration mode. Note that the default E-SBC password is “acme” and the default super user password is “packet”.

```
Password: acme
SBC1> enable
Password: packet
SBC1# configure terminal
SBC1 (configure)#
```

You are now in the global configuration mode.

Initial Configuration – Assigning the management Interface an IP address

To assign an IP address, one has to configure the bootparams on the E-SBC by going to

SBC1#**configure terminal --- >bootparams**

- Once you type “bootparam” you have to use “carriage return” key to navigate down
- A reboot is required if changes are made to the existing bootparams

```
SBC1#(configure)bootparam
'.' = clear field;  '-' = go to previous field;        q = quit boot device              : eth0
processor number        : 0
host name         : acmesystem
file name         : /code/images/nnECZ750p3.bz --- >location where the software is loaded on the SBC
inet on ethernet (e)      : 172.16.1.245:ffffff80 --- > This is the ip address of the management interface of
                            the SBC, type the IP address and mask in hex
inet on backplane (b)   :
host inet (h)     :
gateway inet (g)          : 172.16.1.1->
gateway address here user (u) : vxftp
ftp password (pw) (blank = use rsh)    : vxftp
flags (f)         :
target name (tn)          : SBC1 -> ACLI prompt name & HA peer name
startup script (s)        :
other (o)         :
```

The following section walks you through configuring the Oracle E-SBC. It is outside the scope of this document to include all of the configuration elements as it will differ in every deployment.

Physical Interface:

```
phy-interface
      name                          inside
      operation-type                      Media
      slot                        1
phy-interface
      name                          outside
      operation-type                      Media
```

Network Interfaces:

```
network-interface
      name                          inside
      ip-address                       172.18.1.252
      netmask                          255.255.254.0
      gateway                          172.18.0.1
      hip-ip-list                      172.18.1.252
      icmp-address                         172.18.1.252
network-interface
      name                          outside
      ip-address                       172.18.1.251
      netmask                          255.255.254.0
      gateway                          172.18.0.1
      hip-ip-list                      172.18.1.251
      icmp-address                         172.18.1.251
```

Realms

```
realm-config
      identifier                    inside
      network-interfaces                    inside:0
      mm-in-realm                       enabled
      media-sec-policy                   rtp
realm-config
      identifier                    outside
      network-interfaces                    outside:0
      mm-in-realm                       enabled
      media-sec-policy                   srtp
```

Enable SIP on the SBC and configure default configuration required on the SBC as follows

SIP Config

```
sip-config
    home-realm-id               outside
    registrar-domain             *
    registrar-host             *
    registrar-port             5060
    options                 max-udp-length=0
```

Routing via Local Policy

For outbound calls the local-policy determines which trunk to forward the call based on the NPA of the request-URI. This is configured in the local policy of the “To”. For most configurations there will be only 1 inside and outside realm. For a single inside/outside realm configuration the local policy to and from would be set to “*”. Redundant trunk/Enterprise PBX’s can use a session-agent feature to load balance between servers.

```
local-policy
    from-address                 *
    to-address                 *
    source-realm                 inside
    policy-attribute
        next-hop                  172.18.1.209
        realm                    outside
local-policy
    from-address                 *
    to-address                 *
    source-realm                 outside
    policy-attribute
        next-hop                  172.16.0.62
        realm                    inside
```

Session Agent:

```
session-agent
        hostname                          172.16.0.62
        ip-address                        172.16.0.62
        transport-method                          StaticTCP
        realm-id                        inside
        ping-method                         OPTIONS
        ping-interval                     30
session-agent
        hostname                          172.18.1.209
        ip-address                        172.18.1.209
        port                          5062
        transport-method                          StaticTCP
        realm-id                        outside
        ping-method                         OPTIONS
        ping-interval                     30
session-agent
        hostname                          Anynode
        ip-address                        172.18.1.209
        port                          5063
        state                         disabled
        transport-method                          StaticTLS
        realm-id                        outside
        ping-method                         OPTIONS
        ping-interval                     30
```

Header manipulation rules

Following HMRs were required in order for Oracle ESBC and Anynode device to interoperate.

```
sip-manipulation
        name                              AlterOPTIONS
        header-rule
                name                              AlterOPTIONS
                header-name                               To
                action                            reject
                msg-type                              request
                methods                               OPTIONS
                new-value                              200
```

SIP interface

```
sip-interface
    realm-id                    inside
    sip-port
        address                     172.18.1.252
        transport-protocol               TCP
        allow-anonymous                  agents-only
sip-interface
    realm-id                    outside
    sip-port
        address                     172.18.1.251
        transport-protocol               TCP
        allow-anonymous                  agents-only
    sip-port
        address                     172.18.1.251
        port                      5061
        transport-protocol               TLS
        tls-profile                 SFBTLS
        allow-anonymous                  agents-only
   in-manipulationid             AlterOPTIONS
```

Steering pool config:

The following config needs to be enabled on the SBC in order for the media traffic to traverse thru the SBC.

```
steering-pool
    ip-address                   172.18.1.251
    start-port                  10000
    end-port                    10010
    realm-id                    outside
steering-pool
    ip-address                   172.18.1.252
    start-port                  10020
    end-port                    10030
    realm-id                    inside
```

System configuration:

```
system-config
    default-gateway                 172.18.0.1
    source-routing                 enabled
```

Webserver Configuration

A webserver is available on all Enterprise versions of Oracle E-SBCs. The Webserver can be used to provide tracing, configuration and dashboard info. For tracing info, 2 parts must be configured. 1) The webserver must be enabled. 2) Tracing filters must be applied.

```
web-server-config
    inactivity-timeout              20
```

Enable SIP monitoring:

```
sip-monitoring
```

Enable encryption:

Oracle EBSC can be configured to encrypt both SIP & RTP traffic – with Oracle ESBCs you have the flexibility to encrypt one, both or multiple sides of the call. Following configuration elements were required:

```
certificate-record
    name                        CARoot
    common-name                       SFB-CA
certificate-record
    name                        ToAnynode
    common-name                       172.18.1.251
```

```
media-sec-policy
    name                        srtp
    inbound
        profile                     SDES
        mode                        srtp
        protocol                     sdes
    outbound
        profile                     SDES
        mode                        srtp
        protocol                     sdes
media-sec-policy
    name                        rtp
```

```
tls-global
    session-caching                  enabled
tls-profile
    name                        SFBTLS
    end-entity-certificate            ToAnynode
    trusted-ca-certificates           CARoot
    mutual-authenticate               enabled
    tls-version                  tlsv12
```

Test Plan executed:

Outlook Voice Access (OVA) tests

Outlook Voice Access number:
+4953638195901

Number	Description	Expected Result	Result
1.1.1	Set up call forwarding to OVA on a 3rd party PBX phone. Call this phone from another internal 3rd party PBX phone and wait for the OVA prompt. Leave a message.	OVA plays voice mail greeting. Caller can record a voice message.	[X] Passed [ ] Failed [ ] Untested [ ] MWI set on 3rd party PBX phone
1.1.2	Call OVA from forwarded 3rd party PBX phone.	OVA plays voice access greeting. Enter PIN. Listen to recorded voice message. Delete message.	[X] Passed [ ] Failed [ ] Untested [ ] MWI unset on 3rd party PBX phone
1.1.3	Call the forwarded 3rd party PBX phone from a PSTN / cell phone. Wait for the OVA prompt. Leave a message.	OVA plays voice mail greeting. Caller can record a voice message.	[X] Passed [ ] Failed [ ] Untested [ ] MWI set on 3rd party PBX phone
1.1.4	Call OVA from a PSTN / cell phone. Wait for the OVA prompt. Enter the extension and PIN of the forwarded user.	OVA prompts for extension and PIN. If PIN is correct, OVA plays back recorded message.	[X] Passed [ ] Failed [ ] Untested [ ] MWI unset on 3rd party PBX phone

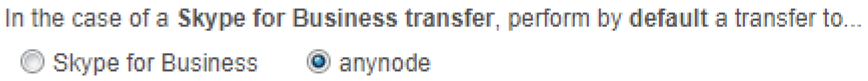
		Delete message.	
1.1.5	Call 3rd party PBX phone from another internal 3rd party PBX phone and wait for the OVA prompt. Do not leave a message.	OVA plays voice mail greeting. Caller can record a voice message. Do not record a message.	[X] Passed [ ] Failed [ ] Untested [ ] MWI not set on 3rd party PBX phone
1.1.6	Call 3rd party PBX phone from another internal 3rd party PBX phone and wait for the OVA prompt. Leave a message.	OVA plays voice mail greeting. Caller can record a voice message.	Continue with next step.
1.1.7	Open the inbox of the forwarded user in Outlook.	Check if the recorded message exists. Play back the message in your browser and on a 3rd party PBX phone. Delete message.	[X] Passed [ ] Failed [ ] Untested [ ] MWI unset on 3rd party PBX phone

Call Transfer via Outlook Voice Access

Outlook Voice Access (OVA) number:
+4953638195901

Transfer call to anynode

On the UCMA node, set this option to anynode:



In the case of a **Skype for Business transfer**, perform by **default** a transfer to...

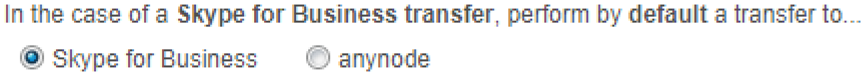
○ Skype for Business ● anynode

Number	Description	Expected Result	Result
1.1.8	Call OVA from	Check if a	[X] Passed

	internal 3rd party PBX phone. Enter two pound signs, followed by the extension of another 3rd party PBX phone: ##xxx Wait for call transfer to complete.	ringback tone is available during call transfer. The 3rd party PBX phones can talk to each other after call transfer has completed.	[ ] Failed [ ] Untested [x] Ringback Tone [x] two-way audio
1.1.9	Call OVA from external PSTN / cell phone. Enter two pound signs, followed by the extension of a 3rd party PBX phone: ##xxx Wait for call transfer to complete.	Check if a ringback tone is available during call transfer. The 3rd party PBX phones can talk to each other after call transfer has completed.	[X] Passed [ ] Failed [ ] Untested [x] Ringback Tone [x] two-way audio

Call Transfer to Skype for Business

On the UCMA node, set this option to Skype for Business:



In the case of a **Skype for Business transfer**, perform by **default** a transfer to...

● Skype for Business ○ anynode

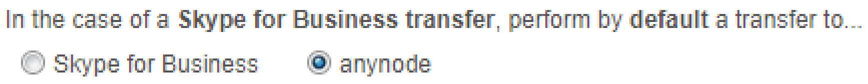
Number	Description	Expected Result	Result
1.1.10	Call OVA from internal 3rd party PBX phone. Enter two pound signs, followed by the extension of another 3rd party PBX phone: ##xxx Wait for call transfer to complete.	Check if a ringback tone is available during call transfer. The 3rd party PBX phones can talk to each other after call transfer has completed.	[X] Passed [ ] Failed [ ] Untested [x] Ringback Tone [x] two-way audio
1.1.11	Call OVA from external PSTN / cell phone. Enter two pound signs, followed by the extension of a 3rd party PBX phone: ##xxx Wait for call transfer to complete.	Check if a ringback tone is available during call transfer. The 3rd party PBX phones can talk to each other after call transfer has completed.	[X] Passed [ ] Failed [ ] Untested [x] Ringback Tone [x] two-way audio

Call Transfer via Outlook Auto Attendant (AA)

Outlook Voice Access (OVA) number:
+4953638195903

Transfer call to anynode

On the UCMA node, set this option to anynode:



In the case of a **Skype for Business transfer**, perform by **default** a transfer to...

○ Skype for Business ● anynode

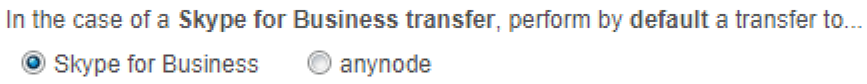
Number	Description	Expected Result	Result
1.1.12	Call AA from internal 3rd party PBX phone. Enter the extension of another 3rd party PBX phone. Wait for call transfer to complete.	Check if a ringback tone is available during call transfer. The 3rd party PBX phones can talk to each other after call transfer has completed.	[X] Passed [ ] Failed [ ] Untested [x] Ringback Tone [x] two-way audio
1.1.13	Call AA from internal 3rd party PBX phone. Enter the extension of a Skype for Business client. Wait for call transfer to complete.	Check if a ringback tone is available during call transfer. The 3rd party PBX phones can talk to each other after call transfer has completed.	[X] Passed [ ] Failed [ ] Untested [x] Ringback Tone [x] two-way audio
1.1.14	Call AA from external PSTN / cell phone. Enter the extension of a 3rd party PBX phone. Wait for call transfer to complete.	Check if a ringback tone is available during call transfer. The 3rd party PBX phones can talk to	[X] Passed [ ] Failed [ ] Untested [x] Ringback Tone [x] two-way audio

		each other after call transfer has completed.	

Number	Description	Expected Result	Result
1.1.15	Call AA from external PSTN / cell phone. Enter the extension of a Skype for Business client. Wait for call transfer to complete.	Check if a ringback tone is available during call transfer. The 3rd party PBX phones can talk to each other after call transfer has completed.	[X] Passed [ ] Failed [ ] Untested [x] Ringback Tone [x] two-way audio

Transfer call to Skype for Business

On the UCMA node, set this option to Skype for Business:



In the case of a **Skype for Business transfer**, perform by **default** a transfer to...

● Skype for Business ○ anynode

Number	Description	Expected Result	Result
1.1.16	Call AA from internal 3rd party PBX phone. Enter the extension of another 3rd party PBX phone. Wait for call transfer to complete.	Check if a ringback tone is available during call transfer. The 3rd party PBX phones can talk to each other after call transfer has completed.	[X] Passed [ ] Failed [ ] Untested [x] Ringback Tone [x] two-way audio
1.1.17	Call AA from internal 3rd party PBX phone. Enter the extension of a Skype for	Check if a ringback tone is available during call	[X] Passed [ ] Failed [ ] Untested

	Business client. Wait for call transfer to complete.	transfer. The 3rd party PBX phones can talk to each other after call transfer has completed.	[x] Ringback Tone [x] two-way audio

Number	Description	Expected Result	Result
1.1.18	Call AA from external PSTN / cell phone. Enter the extension of a 3rd party PBX phone. Wait for call transfer to complete.	Check if a ringback tone is available during call transfer. The 3rd party PBX phones can talk to each other after call transfer has completed.	[X] Passed [ ] Failed [ ] Untested [X] two-way audio
1.1.19	Call AA from external PSTN / cell phone. Enter the extension of a Skype for Business client. Wait for call transfer to complete.	Check if a ringback tone is available during call transfer. The 3rd party PBX phones can talk to each other after call transfer has completed.	[X] Passed [ ] Failed [ ] Untested [x] Ringback Tone [x] two-way audio

Troubleshooting Tools

Wireshark

Wireshark is also a network protocol analyzer which is freely downloadable from www.wireshark.org.

On the Oracle E-SBC

The Oracle E-SBC provides a rich set of statistical counters available from the ACLI, as well as log file output with configurable detail. The follow sections detail enabling, adjusting and accessing those interfaces. Resetting the statistical counters, enabling logging and restarting the log files.

At the E-SBC Console:

```
SBC1# reset sipd
SBC1# notify sipd debug
SBC1#
enabled SIP Debugging
SBC1# notify all rotate-logs
```

ExamALU OXEg the log files

Note: You will FTP to the management interface of the E-SBC with the username user and user mode password (the default is
“acme”

```
C:\Documents and Settings\user>ftp 192.168.1.22
Connected to 192.168.85.55.
220 SBC1 server (VxWorks 6.4) ready. User (192.168.1.22:(none)): user
331 Password required for user. Password: acme
230 User user logged in.
ftp> cd /opt/logs
250 CWD command successful. ftp> get sipmsg.log
200 PORT command successful.
150 Opening ASCII mode data connection for '/opt/logs/sipmsg.log' (3353 bytes).
226 Transfer complete.
ftp: 3447 bytes received in 0.00Seconds 3447000.00Kbytes/sec. ftp> get log.sipd
200 PORT command successful.
150 Opening ASCII mode data connection for '/opt/logs/log.sipd' (204681 bytes).
226 Transfer complete.
ftp: 206823 bytes received in 0.11Seconds 1897.46Kbytes/sec
```

You may now examine the log files with the text editor of your choice.

Through the Web GUI

You can also check the display results of filtered SIP session data from the Oracle Enterprise Session Border Controller, and provides traces in a common log format for local viewing or for exporting to your PC. Please check the “Monitor and Trace” section (page 145) of the Web GUI User Guide available at http://docs.oracle.com/cd/E56581_01/index.htm

Appendix A

Full E-SBC Configuration

```
certificate-record
    name                     CARoot
    common-name                    SFB-CA
certificate-record
    name                     ToAnynode
    common-name                    172.18.1.251
local-policy
    from-address                 *
    to-address                 *
    source-realm                 inside
    policy-attribute
        next-hop                   172.18.1.209
        realm                    outside
local-policy
    from-address                 *
    to-address                 *
    source-realm                 outside
    policy-attribute
        next-hop                   172.16.0.62
        realm                    inside
media-manager
media-policy
    name                     test
media-sec-policy
    name                     srtp
    inbound
        profile                  SDES
        mode                      srtp
        protocol                   sdes
    outbound
        profile                  SDES
        mode                      srtp
        protocol                   sdes
media-sec-policy
    name                     rtp
network-interface
    name                     inside
    ip-address                 172.18.1.252
    netmask                    255.255.254.0
    gateway                 172.18.0.1
    hip-ip-list            172.18.1.252
    icmp-address              172.18.1.252
network-interface
    name                  outside
    ip-address              172.18.1.251
    netmask                 255.255.254.0
    gateway                 172.18.0.1
    hip-ip-list            172.18.1.251
    icmp-address              172.18.1.251
phy-interface
    name                  inside
    operation-type            Media
    slot                 1
phy-interface
    name                  outside
    operation-type            Media
realm-config
    identifier             inside
    network-interfaces          inside:0
    mm-in-realm               enabled
    media-sec-policy           rtp
realm-config
    identifier             outside
    network-interfaces          outside:0
    mm-in-realm               enabled
    media-sec-policy           srtp
sdes-profile
    name                  SDES
session-agent
    hostname                 172.16.0.62
    ip-address              172.16.0.62
    transport-method            StaticTCP
    realm-id               inside
    ping-method               OPTIONS
    ping-interval            30
session-agent
    hostname                 172.18.1.209
    ip-address              172.18.1.209
    port                 5062
    transport-method            StaticTCP
    realm-id               outside
    ping-method               OPTIONS
    ping-interval                  30
session-agent
    hostname                      Anynode
    ip-address                    172.18.1.209
    port                       5063
    state                      disabled
    transport-method                  StaticTLS
    realm-id                     outside
    ping-method                     OPTIONS
    ping-interval                  30
sip-config
    home-realm-id                    outside
    registrar-domain                  *
    registrar-host                 *
    registrar-port                 5060
    options                     max-udp-length=0
sip-interface
    realm-id                     inside
    sip-port
        address                      172.18.1.252
        transport-protocol                TCP
        allow-anonymous                    agents-only
sip-interface
    realm-id                     outside
    sip-port
        address                      172.18.1.251
        transport-protocol                TCP
        allow-anonymous                    agents-only
    sip-port
        address                      172.18.1.251
        port                       5061
        transport-protocol                TLS
        tls-profile                  SFBTLS
        allow-anonymous                    agents-only
    in-manipulationid                 AlterOPTIONS
sip-manipulation
    name                        AlterOPTIONS
    header-rule
        name                        AlterOPTIONS
        header-name                      To
        action                     reject
        msg-type                     request
        methods                      OPTIONS
        new-value                 200
steering-pool
    ip-address                172.18.1.251
    start-port               10000
    end-port                 10010
    realm-id                 outside
steering-pool
    ip-address                172.18.1.252
    start-port               10020
    end-port                 10030
    realm-id                 inside
system-config
    default-gateway              172.18.0.1
    source-routing              enabled
tls-global
    session-caching              enabled
tls-profile
    name                    SFBTLS
    end-entity-certificate        ToAnynode
    trusted-ca-certificates        CARoot
    mutual-authenticate            enabled
    tls-version               tlsv12
web-server-config
    inactivity-timeout           20
```

Appendix B

Accessing the ACLI

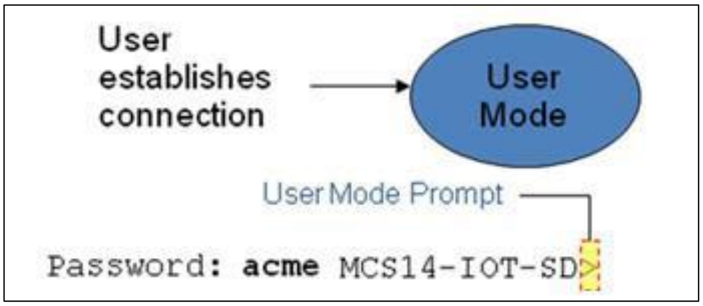
Access to the ACLI is provided by:

- The serial console connection;
- TELNET, which is enabled by default but may be disabled; and
- SSH, this must be explicitly configured.

Initial connectivity will be through the serial console port. At a minimum, this is how to configure the management (eth0) i nterface on the E-SBC.

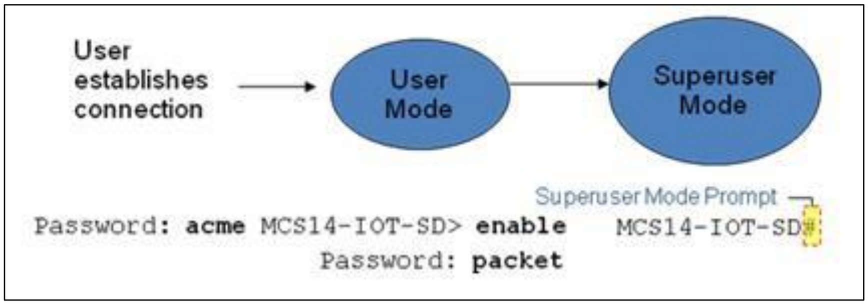
ACLI Basics

There are two password protected modes of operation within the ACLI, User mode and Superuser mode. When you establish a connection to the E-SBC, the prompt for the User mode password appears. The default password is acme. User mode consists of a restricted set of basic monitoring commands and is identified by the greater than sign (>) in the system prompt after the target name. You cannot perform configuration and maintenance from this mode.



```
Password: acme MCS14-IOT-SD>
```

The Superuser mode allows for access to all system commands for operation, maintenance, and administration. This mode is identified by the pound sign (#) in the prompt after the target name. To enter the Superuser mode, issue the enable command i n the User mode.

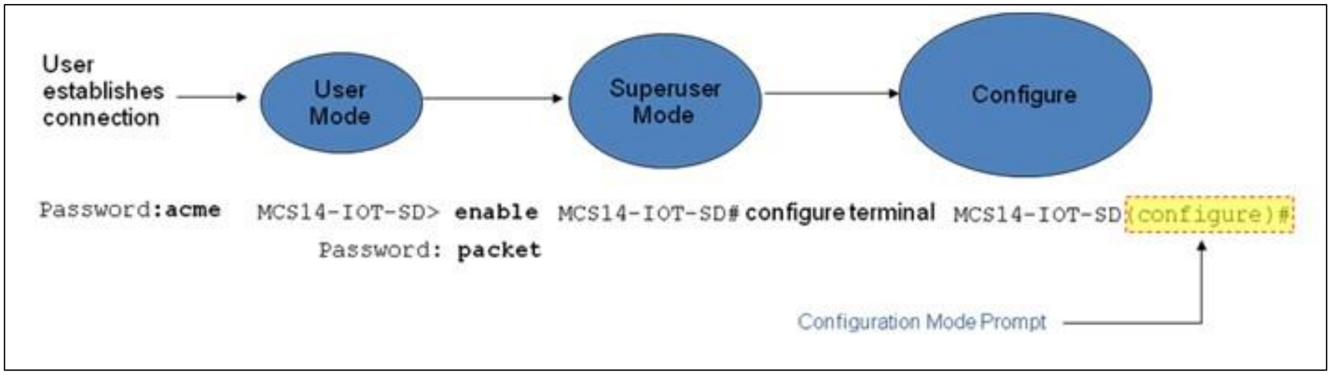


```
Password: acme MCS14-IOT-SD> enable     MCS14-IOT-SD#
                    Password: packet
```

From the Superuser mode, you can perform monitoring and administrative tasks; however you cannot configure any elements. To return to User mode, issue the exit command.

You must enter the Configuration mode to configure elements. For example, you can access the configuration branches and configuration elements for signaling and media configurations. To enter the Configuration mode, issue the configure terminal command in the Superuser mode.

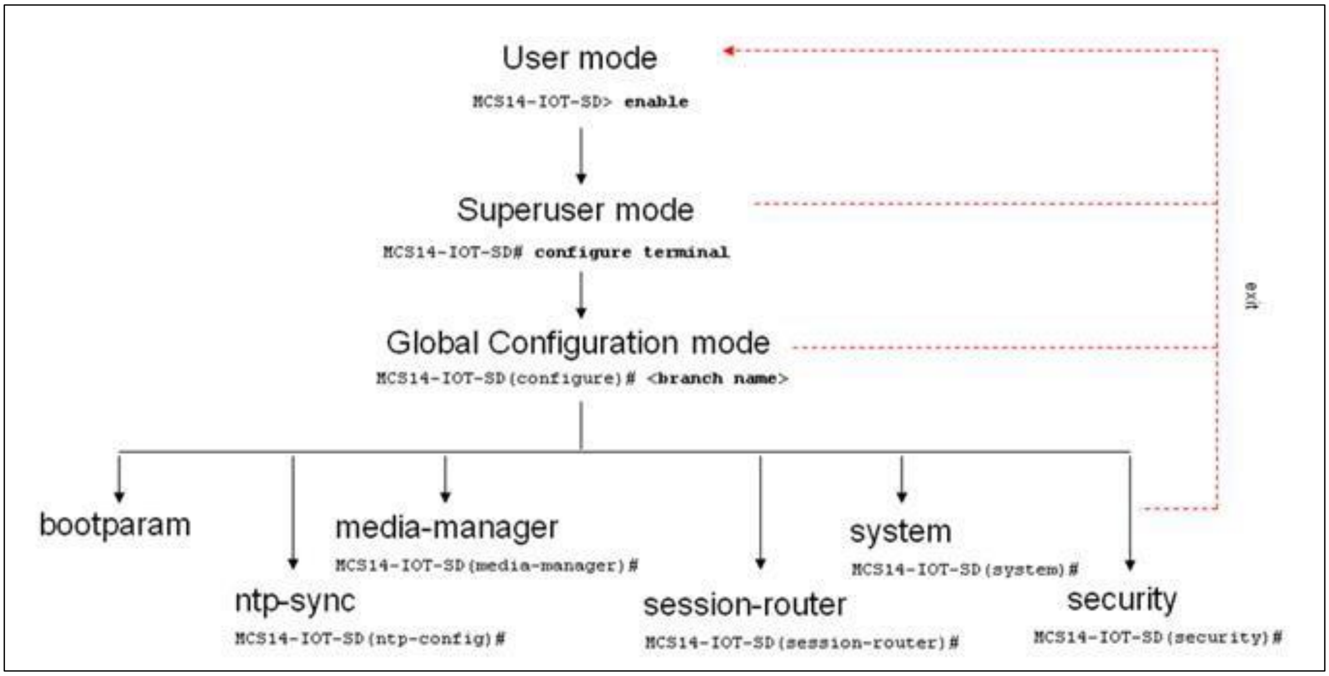
Configuration mode is identified by the word configure in parenthesis followed by the pound sign (#) in the prompt after the target name, for example, SBC1 (configure)#. To return to the Superuser mode, issue the exit command.



```
Password:acme   MCS14-IOT-SD> enable  MCS14-IOT-SD# configure terminal  MCS14-IOT-SD(configure)#
                    Password: packet
```

In the configuration mode, there are six configuration branches:

- bootparam;
- ntp-sync;
- media-manager;
- session-router;
- system; and
- security.



```
MCS14-IOT-SD> enable
MCS14-IOT-SD# configure terminal
MCS14-IOT-SD(configure)# <branch name>
MCS14-IOT-SD(media-manager)#
MCS14-IOT-SD(system)#
MCS14-IOT-SD(ntp-config)#
MCS14-IOT-SD(session-router)#
MCS14-IOT-SD(security)#
```

The ntp-sync and bootparams branches are flat branches (i.e., they do not have elements inside the branches). The rest of the branches have several elements under each of the branches.

The bootparam branch provides access to E-SBC boot parameters. Key boot parameters include:

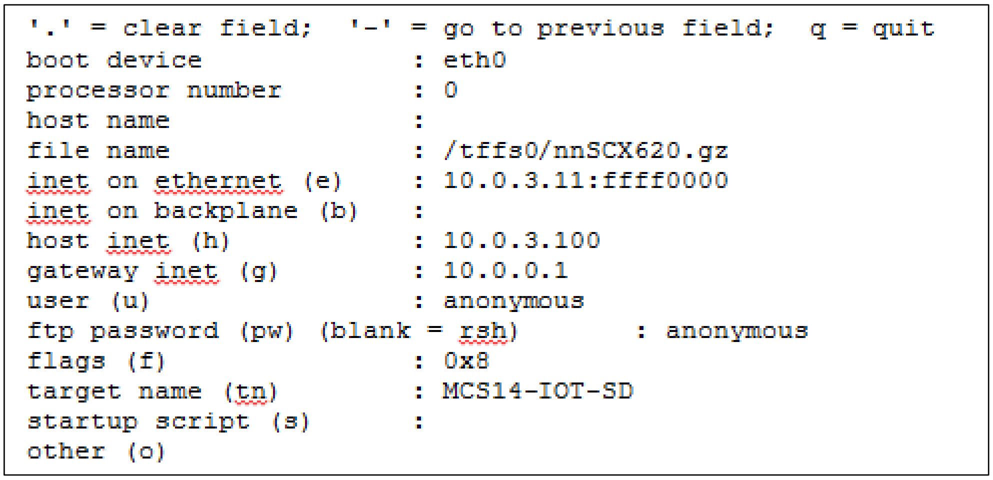
- boot device – The global management port, usually eth0
- file name – The boot path and the image file.

- inet on ethernet – The IP address and subnet mask (in hex) of the management port of the SD.

- host inet –The IP address of external server where image file resides.

- user and ftp password – Used to boot from the external FTP server.

- gateway inet – The gateway IP address for reaching the external server, if the server is located in a different network.



```
'.' = clear field;  '-' = go to previous field;  q = quit
boot device              : eth0
processor number         : 0
host name                :
file name                : /tffs0/nnSCX620.gz
inet on ethernet (e)     : 10.0.3.11:ffff0000
inet on backplane (b)    :
host inet (h)            : 10.0.3.100
gateway inet (g)         : 10.0.0.1
user (u)                 : anonymous
ftp password (pw) (blank = rsh)       : anonymous
flags (f)                : 0x8
target name (tn)         : MCS14-IOT-SD
startup script (s)       :
other (o)
```

The ntp-sync branch provides access to ntp server configuration commands for synchronizing

the E-SBC time and date. The security branch provides access to security configuration.

The system branch provides access to basic configuration elements as system-config, snmp-community, redundancy, physical interfaces, network interfaces, etc.

The session-router branch provides access to signaling and routing related elements, including H323-config, sip-config, iwf-config, local-policy, sip-manipulation, session-agent, etc.

The media-manager branch provides access to media-related elements, including realms, steering pools, dns-config, media- manager, and so forth.

You will use media-manager, session-router, and system branches for most of your working configuration.

Configuration Elements

The configuration branches contain the configuration elements. Each configurable object is referred to as an element. Each element consists of a number of configurable parameters.

Some elements are single-instance elements, meaning that there is only one of that type of the element - for example, the global system configuration and redundancy configuration.

Some elements are multiple-instance elements. There may be one or more of the elements of any given type. For example, physical and network interfaces.

Some elements (both single and multiple instance) have sub-elements. For example:

- SIP-ports - are children of the sip-interface element

- peers – are children of the redundancy element

- destinations – are children of the peer element

Creating an Element

1. To create a single-instance element, you go to the appropriate level in the ACLI path and enter its parameters. There is no need to specify a unique identifier property because a single-instance element is a global element and there is only one instance of this element.
2. When creating a multiple-instance element, you must specify a unique identifier for each instance of the element.
3. It is important to check the parameters of the element you are configuring before committing the changes. You do this by issuing the show command before issuing the done command. The parameters that you did not configure are filled with either default values or left empty.
4. On completion, you must issue the done command. The done command causes the configuration to be echoed to the screen and commits the changes to the volatile memory. It is a good idea to review this output to ensure that your configurations are correct.
5. Issue the exit command to exit the selected element.

Note that the configurations at this point are not permanently saved yet. If the E-SBC reboots, your configurations will be lost.

Editing an Element

The procedure of editing an element is similar to creating an element, except that you must select the element that you will edit before editing it.

- Enter the element that you will edit at the correct level of the ACLI path.

- Select the element that you will edit, and view it before editing it.
- The select command loads the element to the volatile memory for editing. The show command allows you to view the element to ensure that it is the right one that you want to edit.
- Once you are sure that the element you selected is the right one for editing, edit the parameter one by one. The new value you provide will overwrite the old value.
- It is important to check the properties of the element you are configuring before committing it to the volatile memory. You do this by issuing the show command before issuing the done command.
- On completion, you must issue the done command.
- Issue the exit command to exit the selected element.

Note that the configurations at this point are not permanently saved yet. If the E-SBC reboots, your configurations will be lost.

Deleting an Element

The no command deletes an element from the configuration in editing. To delete a single-instance element,

- Enter the no command from within the path for that specific element
- Issue the exit command. To delete a multiple-instance element,

- Enter the no command from within the path for that particular element.
- The key field prompt, such as <name>:<sub-port-id>, appears.
- Use the <Enter> key to display a list of the existing configured elements.
- Enter the number corresponding to the element you wish to delete.
- Issue the select command to view the list of elements to confirm that the element was removed.

Note that the configuration changes at this point are not permanently saved yet. If the E-SBC reboots, your configurations will be lost.

Configuration Versions

At any time, three versions of the configuration can exist on the E-SBC: the edited configuration, the saved configuration, and the running configuration.

- The edited configuration – this is the version that you are making changes to. This version of the configuration is stored in the E-SBC's volatile memory and will be lost on a reboot.
- To view the editing configuration, issue the show configuration command
- The saved configuration – on issuing the save-config command, the edited configuration is copied into the non- volatile memory on the E-SBC and becomes the saved configuration. Because the saved configuration has not been activated yet, the changes in the configuration will not take effect. On

reboot, the last activated configuration (i.e., the last running configuration) will be loaded, not the saved configuration.

- The running configuration is the saved then activated configuration. On issuing the activate-config command, the saved configuration is copied from the non-volatile memory to the volatile memory. The saved configuration is activated and becomes the running configuration. Although most of the configurations can take effect once being activated without reboot, some configurations require a reboot for the changes to take effect.
- To view the running configuration, issue command show running-config.

Saving the Configuration

The save-config command stores the edited configuration persistently.

Because the saved configuration has not been activated yet, changes in configuration will not take effect. On reboot, the las t activated configuration (i.e., the last running configuration) will be loaded. At this stage, the saved configuration is different from the running configuration.

Because the saved configuration is stored in non-volatile memory, it can be accessed and activated at later time.

Upon issuing the save-config command, the E-SBC displays a reminder on screen stating that you must use the activate- config command if you want the configurations to be updated.

```
SBC1 # save-config
Save-Config received, processing. waiting 1200
for request to finish Request to 'SAVE-CONFIG'
has Finished, Save complete
Currently active and saved configurations do not match!
To sync & activate, run 'activate-config' or 'reboot activate'.
SBC1
```

Activating the Configuration

On issuing the activate-config command, the saved configuration is copied from the non-volatile memory to the volatile memory. The saved configuration is activated and becomes the running configuration.

Some configuration changes are service affecting when activated. For these configurations, the E-SBC warns that the change could have an impact on service with the configuration elements that will potentially be service affecting. You may decide whether or not to continue with applying these changes immediately or to apply them at a later time.

```
SBC1# activate-config Activate-Config
received, processing. waiting 120000 for
request to finish Request to 'ACTIVATE-
CONFIG' has Finished, Activate Complete
SBC1#
```

ORACLE

Oracle Corporation, World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200

CONNECT WITH US

blogs.oracle.com/oracle
facebook.com/oracle
twitter.com/oracle
oracle.com

Integrated Cloud Applications & Platform Services